Baylor University: Delivering secure broadband access

Overview

- ***Business Challenge***
  Baylor University sought to prevent potentially crippling network outages due to phishing, spamming and botnet attacks, as well as from intentional misuse. To support its ongoing efforts, Baylor needed tools to help its administrators continually monitor the behavior of users, networks and applications across the entire university.
- ***Solution***
  The university chose IBM Proventia® Network Anomaly Detection System to deliver a clear view of network broadband behavior while automatically detecting active security threats, risky user behavior, performance issues, policy violations and unapproved changes.
- ***Key Benefits***
  - *Ability to monitor ports, services and applications to quickly identify the root cause of unusual activity*
  - *Provides 100 percent transparency into issues affecting bandwidth and traffic flow*
  - *Easily manage firewall policy and enhance ability to defend against diverse threats*

Enhanced transparency for quick issue resolution

Baylor University in Waco, Texas, provides more than 14,000 students wireless broadband Internet access across its 735-acre campus. Baylor's challenge was to address threats, safeguard sensitive information and to protect Baylor's reputation by supplementing the existing protections and adding a tool to enable behavioral analysis of the internal network.

The university was already successfully using The IBM Proventia Network Intrusion Prevention System (IPS) to prevent security breaches and stop malicious Internet attacks. To prevent evolving threats, such as internal misuse, phishing, botnets or propagating worms – all of which can inhibit a high-performing network, Baylor decided to implement the IBM Proventia Network Anomaly Detection System.

> *"We've enjoyed a more complete view of the Baylor broadband network than we've ever had before – which not only improves security, but helps us to enhance the health of the network overall and the services we deliver to our user base."*
>
> – Jon Allen, information security officer, Baylor University

"Prior to the implementation," says Jon Allen, information security officer at Baylor, "We would spend days investigating issues which now can be answered in a few seconds. For example, we recently had a spear phishing attack. With our new tools, the phisher was quickly identified and blocked from doing any damage." Hackers have been known to send thousands of fraudulent e-mails from university addresses, taxing network resources and reducing user confidence in security. However, once alerted by the system, Baylor was able to easily deny access to the attacker, without causing bottlenecks or requiring network redesign.

When a problem arises, Baylor's information security team now has instant credibility with other administrators. Because the system audits the flow of data across the entire network, the level of detail supplied makes it easy for the team to cross departmental lines. "When we identify suspicious activity that originated on the e-mail server, for example, we can narrow it down to a specific IP address and a specific time frame, present that information to the e-mail administrator, who can then take the appropriate action," explains Adam Sealey, information security analyst, Baylor University.

Defending data and preventing outages

Baylor sees three distinct areas of value in the IBM Proventia Network Anomaly Detection System: security, compliance/corporate governance and networking operations. "We've been able to spotlight misuse and monitor attacks and virus outbreaks by identifying behaviors that differed from the norm," says Sealey.

Sealey notes that students are apt to download anything presented to them. "Before, measuring compliance with acceptable use was difficult," he continues. "Now, we can use custom rules to shape the system and monitor proper usage at Baylor. The transparency it provides makes it very easy to spot when users go beyond acceptable behavior."

Baylor also finds that the product suite is ideally suited to help identify the root cause of outages, and to perform ad-hoc research and analysis. The university is now able to refine its network to address any issues, thanks to the forensic log of activity which provides 100 percent visibility to services, servers and clients.

The Baylor team initially used the protection products as part of a beta program, becoming the first university to implement advanced tools of this kind. As a veteran beta tester for various providers, Allen asserts that: "The beta tools were ready for heavy usage from day one, and the IBM team remains extremely responsive and helpful with any questions we've had along the way."

For more information

To learn more about how IBM can help you to secure data and safeguard sensitive information, please contact your IBM representative or IBM Business Partner.

Visit us at:

ibm.com/innovation

IBM Corporation
1 New Orchard Road
Armonk, NY 10504
U.S.A.

Produced in the United States of America
8-08

ODC03083-USEN-00